VersaSense

Introduction to MicroPnP

Danny Hughes
info@versasense.com

Dust Consortium, Tokyo, 27/10/2016

Structure of this talk

Part 1 - MicroPnP Products

Part 2 - Certified Security

Part 3 - Plug and play sensing

Structure of this talk

Part 1 - MicroPnP Products

Part 2 - Certified Security

Part 3 - Plug and play sensing

Key Differetiators

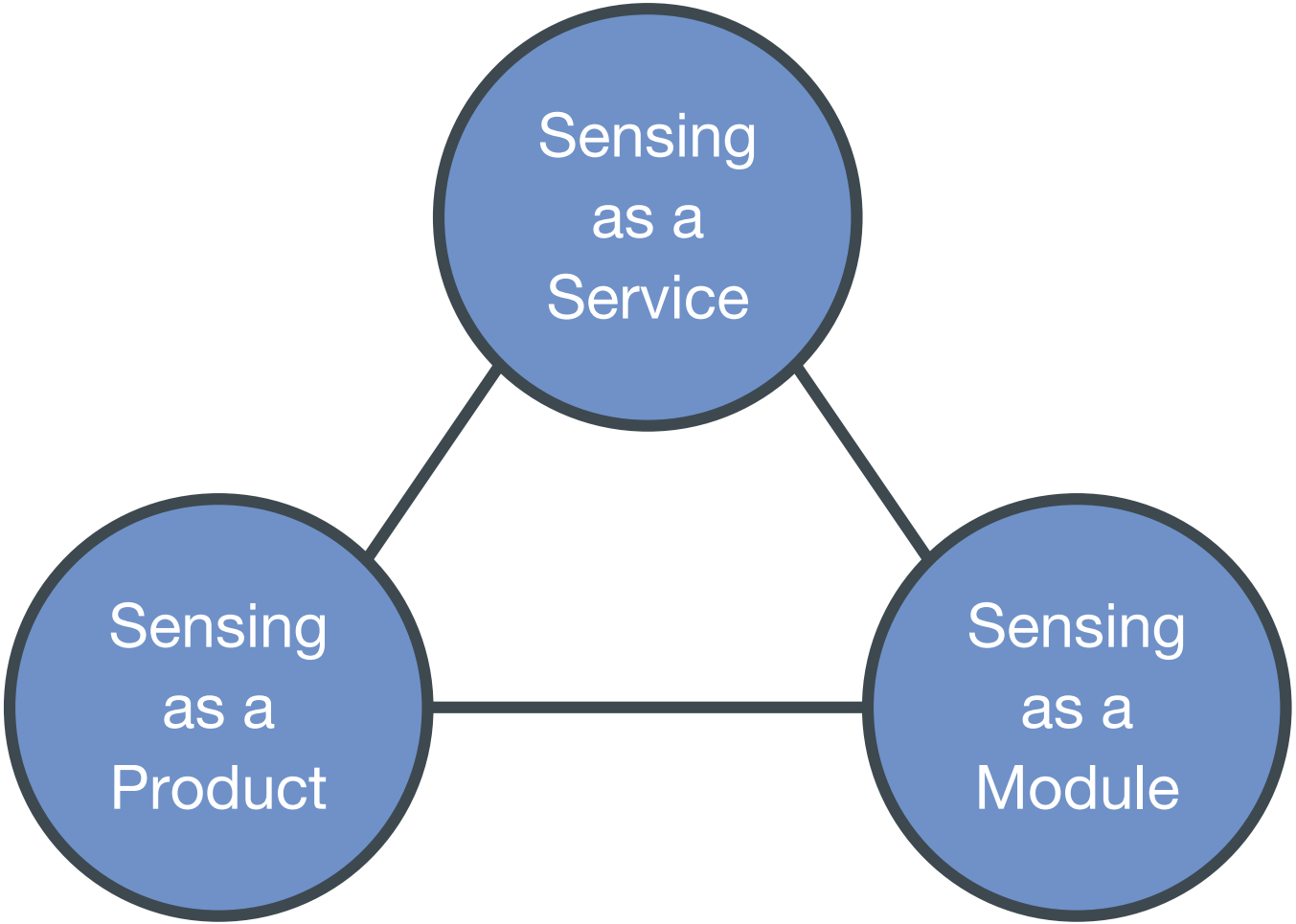
Zero-configuration
plug-and-play customization

99.999% wireless network
reliability

Up to 10 years
battery life

100% based on
open standards

World most secure
commissioning solution.


Sensing as a Service
Sensing as a Product
Sensing as a Module

Structure of this talk

Part 1 - MicroPnP Products

Part 2 - Certified Security

Part 3 - Plug and play sensing

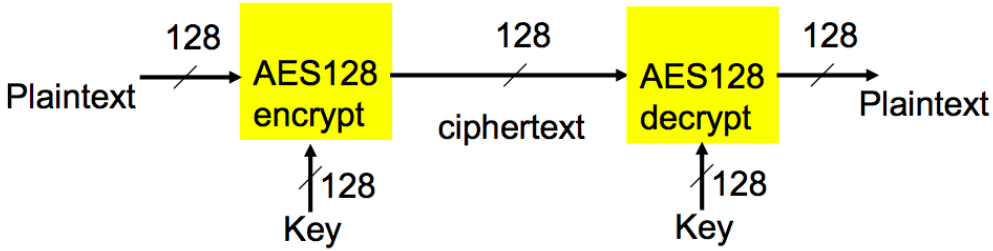
Network Security Essentials

- **Encryption:** make sure that no one can see the data
- **Integrity:** avoid forged, replayed & corrupt packets
- **Authentication:** join only trusted networks
- **Commissioning:** join only *the right* trusted network.

Secure Routing in SmartMesh-IP

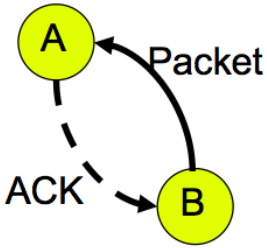
On Send:

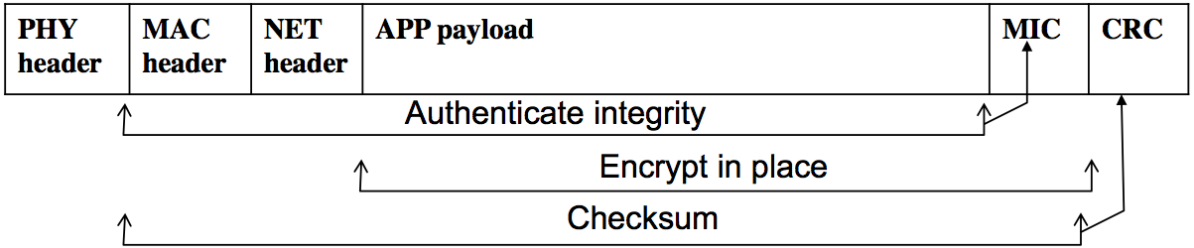
- Authenticate data and headers with MIC
- Encrypt payload and headers.
- Append aCRC checksum



On receive:

- Verify CRC to remove corrupted packets
- Decrypt payload, MIC
- Verify message integrity





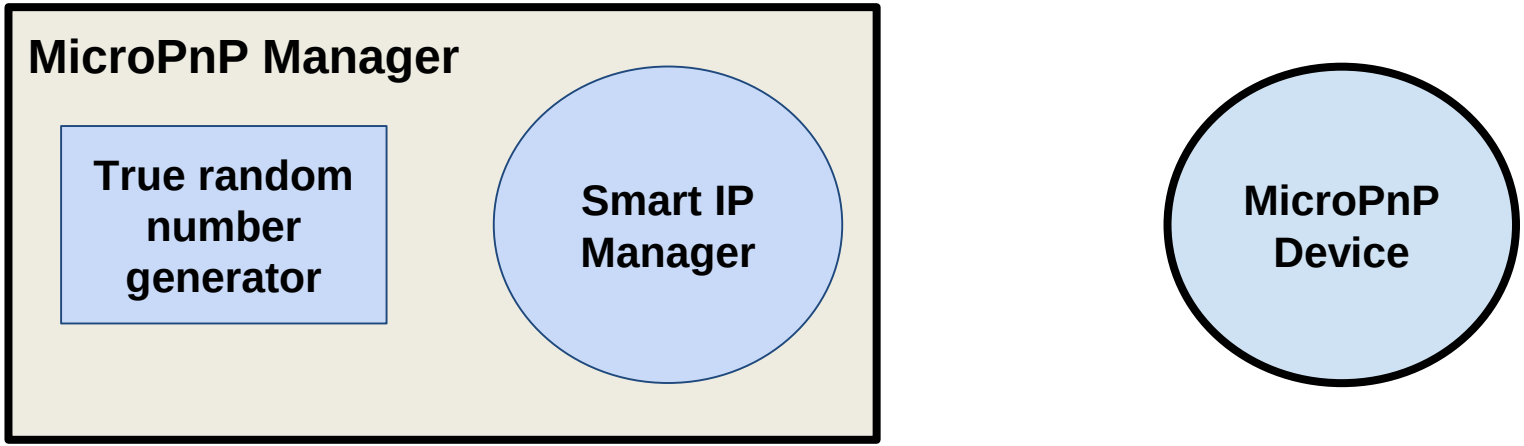
Key Distribution Schemes

TYPE	DESCRIPTION
(a) Single shared network key	**Unacceptable:** shared key must be considered compromised. This gives attackers full access to everything.
(b) Shared join key, unique session key	**Industry standard:** join key must be considered compromised. Compromise allows attackers to sniff session keys for any node.
(c) Unique join key and session key	**Google thread:** there are no common keys to compromise, but Google manages all keys.

Unique Security Approach

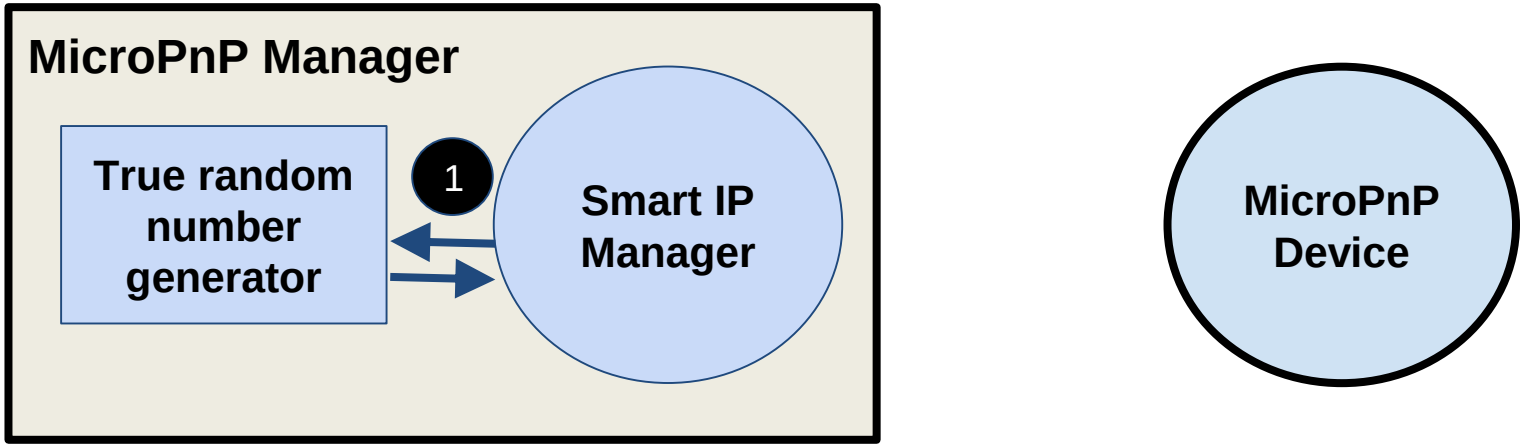
- **Eliminates key management complexity** allowing plug-and-play commissioning of MicroPnP devices.
- **Eliminates shared join keys**, to prevent widespread sniffing of the motes' session keys.
- **Clients have complete control** over the security of their network, with no 3rd-party key management.

High Security Comissioning



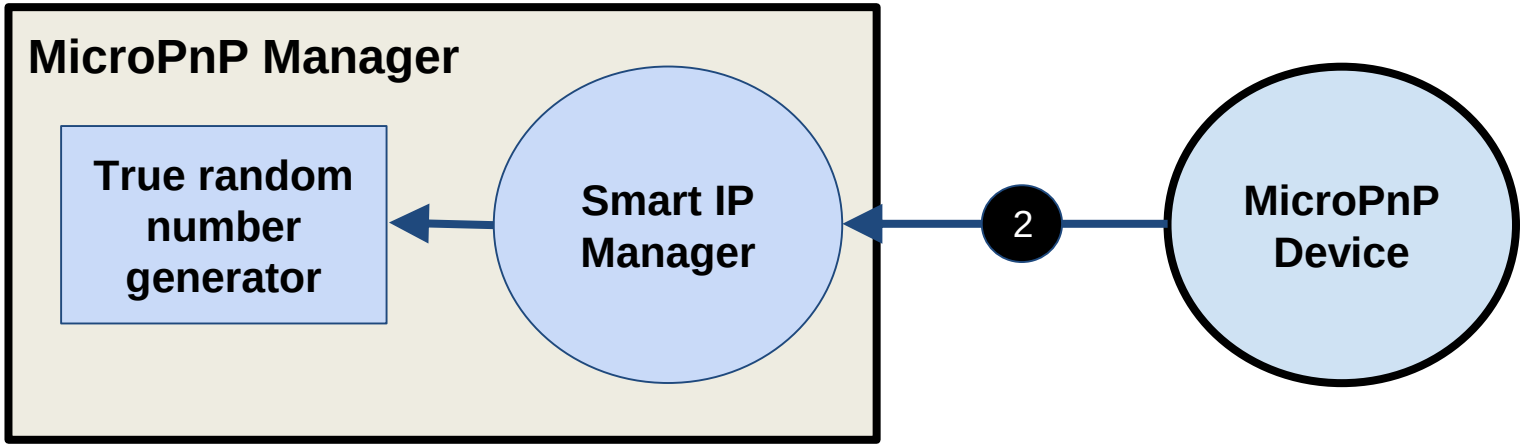
NIST-certified random number generator (RNG) creates secret keys on site. **No 3rd party stores keys / IDs.**

High Security Comissioning



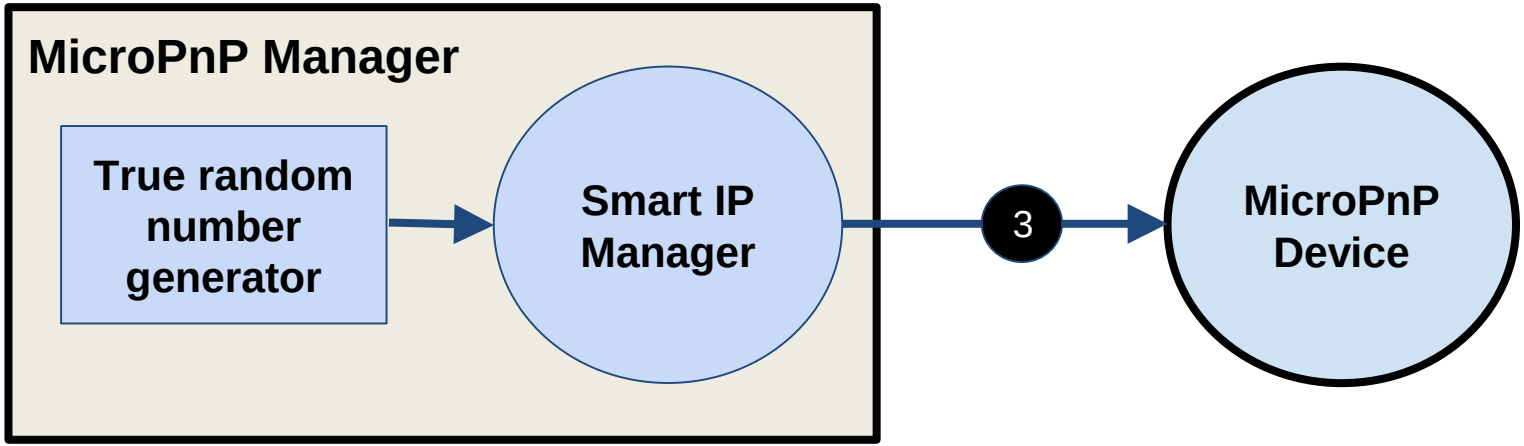
(1) RNG creates unique Smart Mesh network ID upon first power-up.

High Security Comissioning



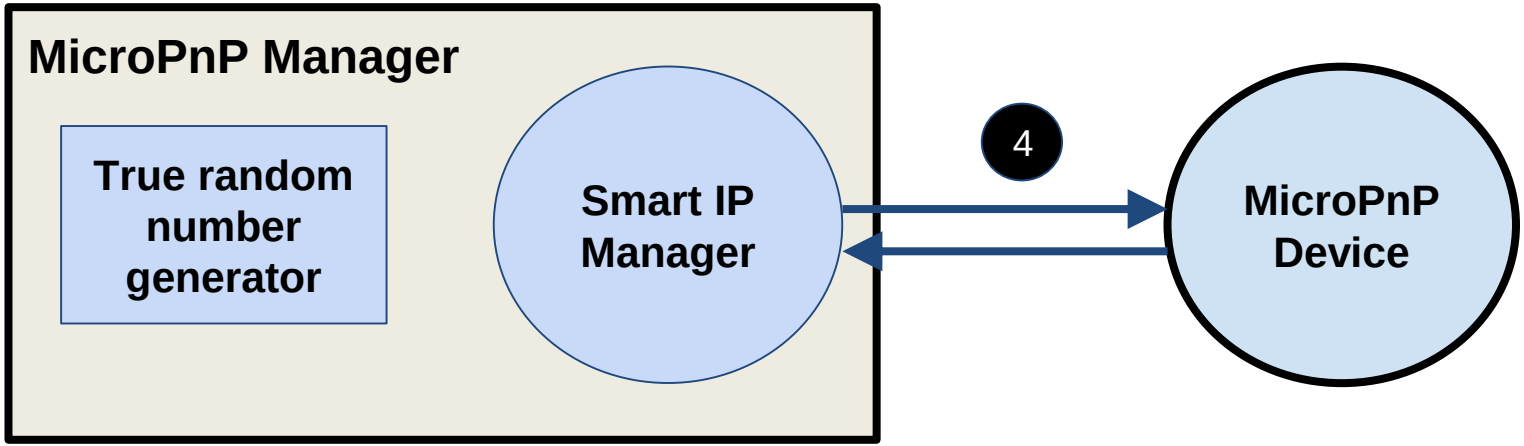
(2) Factory-fresh MicroPnP device is plug-and-play connected to manager, or installer PC via wired interface.

High Security Comissioning



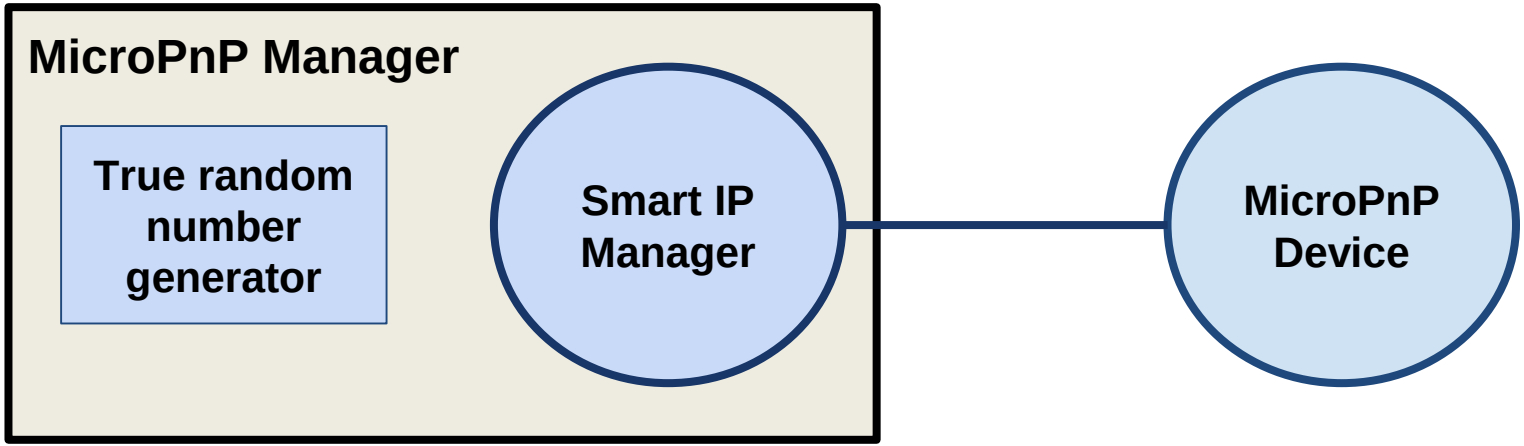
(3) Unique join key is created and sent to device, which is added to access control list of the manager.

High Security Comissioning



(4) Device requests session keys from manager using unique join key and NIST-certified AES-128 security.

High Security Comissioning



MicroPnP achieves **end-to-end NIST certified security**, with no third party storage of clients data or keys.

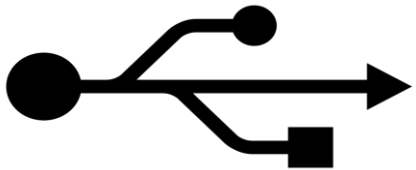
Structure of this talk

Part 1 - MicroPnP Products

Part 2 - Certified Security

Part 3 - Plug and play sensing

Inspired by Mainstream Systems



How can we identify, discover and use peripherals at extreme low cost?

Live Demonstration

http://versa-gw.local